IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2 CONTROLLING A COMPUTER NETWORK THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS,

Defendants.

Civil Action No: 1:20CV730 CMH/JFA

FILED UNDER SEAL PURSUANT TO LOCAL CIVIL RULE 5

COMPLAINT

This is an action to stop cybercriminals from exploiting the COVID-19 pandemic in an attempt to unlawfully obtain access to personal and confidential information of Microsoft customers. Specifically, Defendants in this action are part of an online criminal network whose tactics evolved to take advantage of global current events by deploying a COVID-19 themed phishing campaign targeting Microsoft customers around the world. This sophisticated phishing campaign is designed to compromise thousands of Microsoft customer accounts and gain access to customer email, contact lists, sensitive documents, and other personal information. All in an attempt to exfiltrate information, re-direct wire transfers, and launch further cybercrime from compromised accounts. The relief sought in this action is necessary to stop irreparable and ongoing harm to Microsoft and its customers.

Plaintiff Microsoft Corporation ("Microsoft") hereby complains and alleges that John Does 1-2 (collectively "Defendants") send phishing emails containing deceptive messages concerning the global COVID-19 pandemic or other socially engineered lures in order to induce

targeted victims to click on malicious links in those emails. These phishing emails are designed to look like they come from an employer or other trusted source. Defendants misuse Microsoft's name and trademarks to further induce victims to click the links and interact with malicious software. Egregiously capitalizing on a public health crisis, through these schemes, Defendants attempt to gain unauthorized access to victims' Microsoft Office 365 accounts. Internet domains used by Defendants to carry out this criminal scheme are set forth at **Appendix A** to this Complaint, and referred to as the "Malicious Infrastructure." Microsoft alleges as follows:

NATURE OF THE ACTION

1. This is an action based upon: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.*; (3) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (4) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (5) Trespass to Chattels; (6) Conversion, and (7) Unjust Enrichment. Plaintiff seeks injunctive and other equitable relief and damages against Defendants who, through their illegal activities, have caused and continue to cause irreparable injury to Microsoft, its customers, and the public.

PARTIES

2. Plaintiff Microsoft is a corporation duly organized and existing under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington.

3. On information and belief, John Doe 1 controls the Malicious Infrastructure in furtherance of conduct designed to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 1 can likely be contacted

directly or through third-parties using the information set forth in **Appendix A**.

4. On information and belief, John Doe 2 controls the Malicious Infrastructure in furtherance of conduct designed to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 2 can likely be contacted directly or through third-parties using the information set forth in **Appendix A**.

5. Third parties Verisign, Inc., Verisign Information Services, Inc., and Verisign Global Registry Services (collectively, "Verisign") are the domain name registry entities that oversee the registration of all domain names ending in ".com," including the domains used by Defendants. Verisign is located at 12061 Bluemont Way, Reston, Virginia 20190, United States.

6. On information and belief, Defendants jointly own, rent, lease, or otherwise have dominion over the Malicious Infrastructure used to carry out the cyberattacks that are the subject of this complaint. Microsoft will amend this complaint to allege the Defendants' true names and capacities when ascertained. Microsoft will exercise due diligence to determine Defendants' true names, capacities, and contact information, and to effect service upon those Defendants.

7. Microsoft is informed and believes and thereupon alleges that each of the fictitiously named Defendants is responsible in some manner for the occurrences herein alleged, and that Microsoft's injuries as herein alleged were proximately caused by such Defendants.

8. On information and belief, the actions and omissions alleged herein to have been undertaken by Defendants were actions that they, and each of them, authorized, controlled, directed, or had the ability to authorize, control or direct, and/or were actions and omissions each Defendant assisted, participated in, or otherwise encouraged, and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions and omissions of Defendants set forth below, in that each Defendant had knowledge of those actions and omissions, provided

assistance and benefited from those actions and omissions, in whole or in part. Each Defendant was the agent of each of the remaining Defendants, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of other Defendants.

JURISDICTION AND VENUE

9. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises out of Defendants' violation of The Computer Fraud and Abuse Act (18 U.S.C. § 1030) and the Lanham Act (15 U.S.C. §§ 1114, 1125). The Court also has subject matter jurisdiction over Microsoft's claims for trespass to chattels, conversion, and unjust enrichment pursuant to 28 U.S.C. § 1367.

10. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Microsoft's claims has occurred in this judicial district, because a substantial part of the property that is the subject of Microsoft's claims is situated in this judicial district, and because a substantial part of the harm caused by Defendants has occurred in this judicial district. Defendants maintain internet domains registered in Virginia, engage in other conduct availing themselves of the privilege of conducting business in Virginia, and utilize instrumentalities located in Virginia and the Eastern District of Virginia to carry out acts alleged herein. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are subject to personal jurisdiction in this judicial district.

11. Defendants have affirmatively directed actions at Virginia and the Eastern District of Virginia by directing their activities, including theft of information, at victims located in the Eastern District of Virginia.

12. Defendants' Malicious Infrastructure, particularly domain names, is registered

through Verisign which resides in the Eastern District of Virginia. Defendants use these domains to communicate with and control malicious applications that target Microsoft and its customers. Defendants have undertaken the acts alleged herein with knowledge that such acts would cause harm through domains located in and maintained through facilities in the Eastern District of Virginia, targeting customers in the Eastern District of Virginia and elsewhere in the United States, thereby injuring Microsoft and its customers. Therefore, this Court has personal jurisdiction over Defendants.

13. Defendants have directed their relevant activity to targeted victims in, among other places, Alexandria, Arlington, Chantilly, McLean, Falls Church, Herndon and Reston as included in the map at **Figure 1** below.

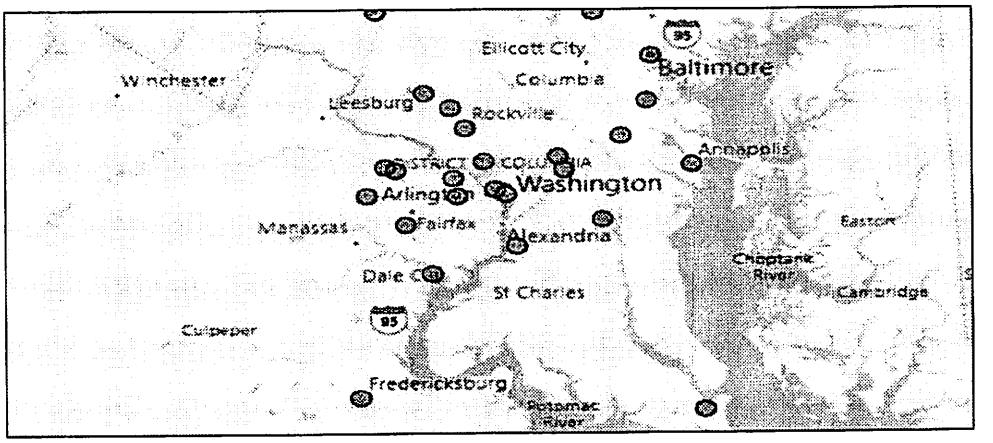

Figure 1

FACTUAL BACKGROUND

Microsoft's Services and Reputation

14. Microsoft® is a provider of the Office 365,® OneDrive,® and SharePoint® cloud-based business and productivity suite of services, all offered under those trademarks and in connection with the Microsoft mark and the Microsoft corporate logo. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality

and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Microsoft, Office 365, OneDrive and SharePoint trademarks. Copies of the trademark registrations are attached as **Appendix B** to this Complaint.

Summary of Defendants' Illegal Activity

15. Defendants send phishing emails containing deceptive messages concerning the global COVID-19 pandemic in order to induce targeted victims to click on malicious links in those emails. These phishing emails are designed to look like they come from an employer or other trusted source. Once the victims click on the malicious links, they are led to servers which present the victims with a malicious Web Application ("Web App").[1] The malicious Web App interacts with Microsoft's Office 365 services. Having convinced the victims that the original phishing email was sent by a trusted source, the criminals then cause the victims to erroneously believe that the Web App also originates from the same trusted source and, most importantly, is approved or published by Microsoft. As a result, targeted victims are deceived into clicking a button that grants the malicious Web App, and therefore the criminals, access to the victims' Office 365 account including the account contents, such as email, contacts, notes and material stored in the victims' OneDrive for Business cloud storage space and corporate SharePoint

[1] For clarity, the references here to a "Web App" do not relate to mobile apps. Rather, the Web App is software running on servers controlled by Defendants and which can interact with and obtain access to Microsoft Office 365 accounts.

document management and storage system. The attacker may also be able to access and alter account settings as the attacker has full control over the account. Until the Web App is disabled or token revoked, the attacker will have continued access to the Office 365 account.

16. In this way, the attackers attempt to gain unauthorized access to Office 365 accounts of Microsoft's customers. Notably, this scheme enables unauthorized access without explicitly requiring the victims to directly give up their login credentials at a fake website or similar interface. Rather, the victims input their credentials into legitimate Office 365 login pages that are not under the cybercriminals' control. In some instances, the victim may alternatively be asked to confirm the identity linked to their device in lieu of entering credentials. Thereafter, the cybercriminals utilize the malicious Web Apps to gain access based on the victims' previous entry of credentials. This highly deceptive scheme has the same practical effect as direct theft of credentials, except that the victims are not aware that they unintentionally provided cybercriminals access to their Office 365 account.

17. Microsoft commits tremendous resources to detecting and blocking threats to its customers and their accounts. In December 2019, Microsoft first detected early instances of the Defendants' malicious phishing and Web App scheme and began collecting information regarding Defendants' creation and deployment of the malicious Web Apps and known attempts by the Web Apps to access Microsoft's cloud infrastructure. Based on patterns discovered at that time, Microsoft developed technical means to block the Defendants' activity and disabled the Web Apps that existed at that time. In this way, Microsoft was, thus far, able to protect its customers. However, recently Defendants have begun creating new malicious Web Apps. Defendants' activities pose a persistent risk. Defendants have sent millions of phishing emails. Defendants continue to evolve their tactics, now leveraging messages purporting to be about

important COVID-19 issues. Defendants have designed these COVID-19-themed phishing emails, like the previous emails, to deceive recipients to click on a link and thereafter grant access to their Office 365 accounts via new versions of the malicious Web Apps.

18. Defendants attempted to target Microsoft customers in both the private and public sectors, including businesses in different industries. Defendants frequently targeted the C-suite, senior managers, and regional leaders of a variety of businesses and organizations.

Defendants Use Deceptive COVID-19 Messages and Malicious Web Apps in an Attempt to Compromise Office 365 Accounts

19. Defendants send phishing emails to Microsoft's customers who are using its Office 365 email service. Defendants design these emails in a manner that deceptively impersonates legitimate communications originating from Microsoft's SharePoint or OneDrive for Business cloud storage services. For example, in these emails, Defendants leverage the presence of the "Microsoft" and "OneDrive" trademarks, and the presence of the term "SharePoint" in the "From" email address to convince recipients that this is a legitimate communication from Microsoft. Further, Defendants send phishing emails from email addresses that contain references to companies or entities associated with the recipient, such as the name of their employer. Defendants may send phishing emails from compromised accounts of parties, such as employers or colleagues, within the recipient's trusted network.

20. Defendants also include in the phishing emails other deceptive content, usually what appears to be a link to "Open" a Microsoft Excel document. In fact, as detailed further below, this icon in the email is a malicious link that begins the process of Defendants attempting to obtain access to the victims' Office 365 accounts. Because victims are usually familiar and experienced with the legitimate file-share method using OneDrive for Business or SharePoint, and because the email appears to originate from a trusted entity (such as an employer) and

contains typical data that might appear in a legitimate file-sharing email, the victims are tricked into clicking the malicious link.

21. When Defendants first began carrying out this scheme, the phishing emails contained deceptive themes associated with generic business activity. For example, the malicious Excel link would be named in a manner that uses information suggesting it is associated with a trusted entity and business terms such as "Q4 Report – Dec19." An example of an earlier phishing email is reproduced as **Figure 2**. Specific information has been redacted here to protect the privacy of potential victims.

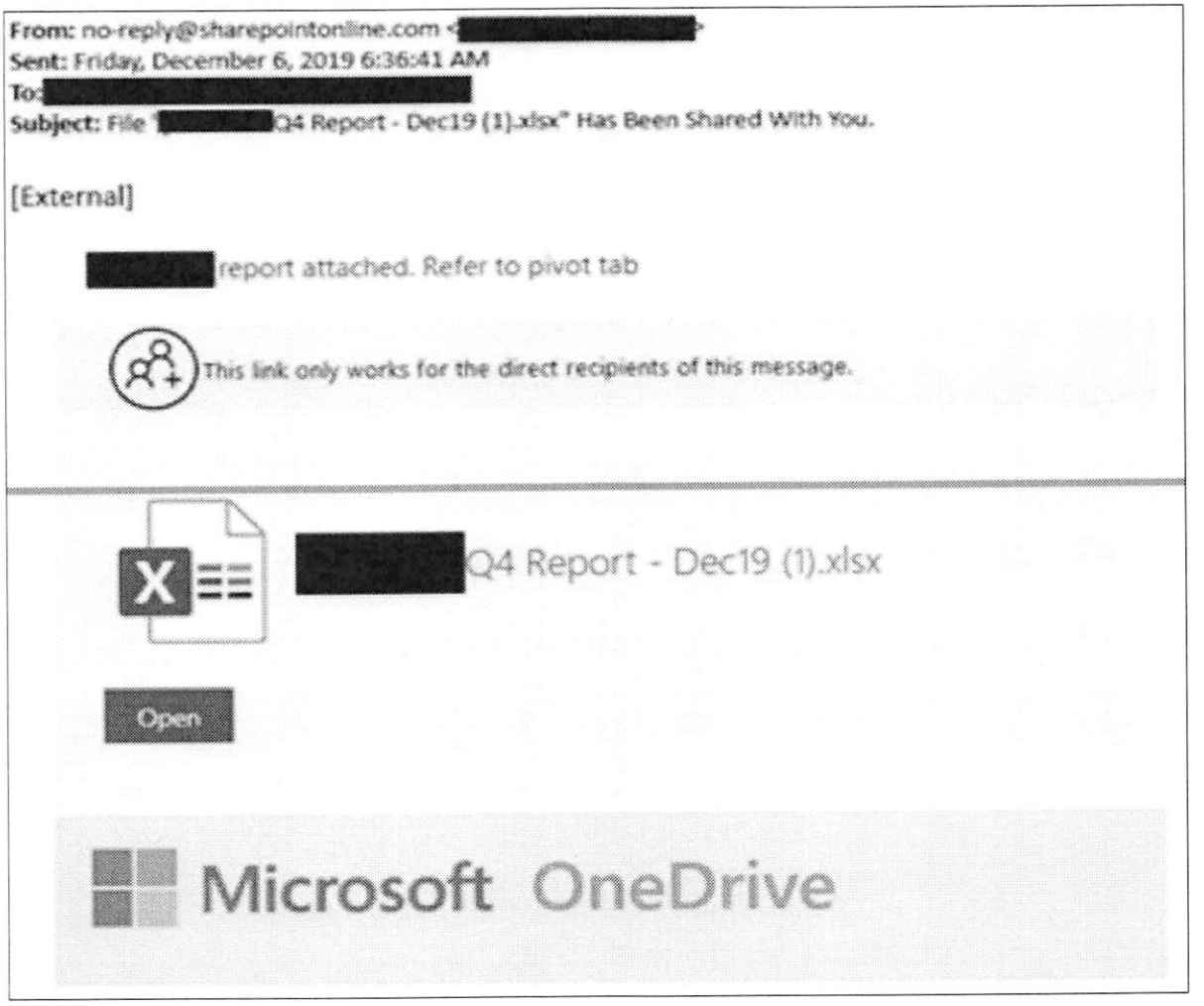

Figure 2

22. Recently, as Defendants have renewed their efforts to target Microsoft and its customers, Defendants have created phishing emails containing deceptive themes associated with COVID-19. For example, Defendants now name the malicious Excel link in a manner suggesting it is associated with a trusted entity and use terms such as "COVID-19 Bonus." An example of such a COVID-19 related phishing email is reproduced as **Figure 3**. Specific information has been redacted here to protect the privacy of potential victims.

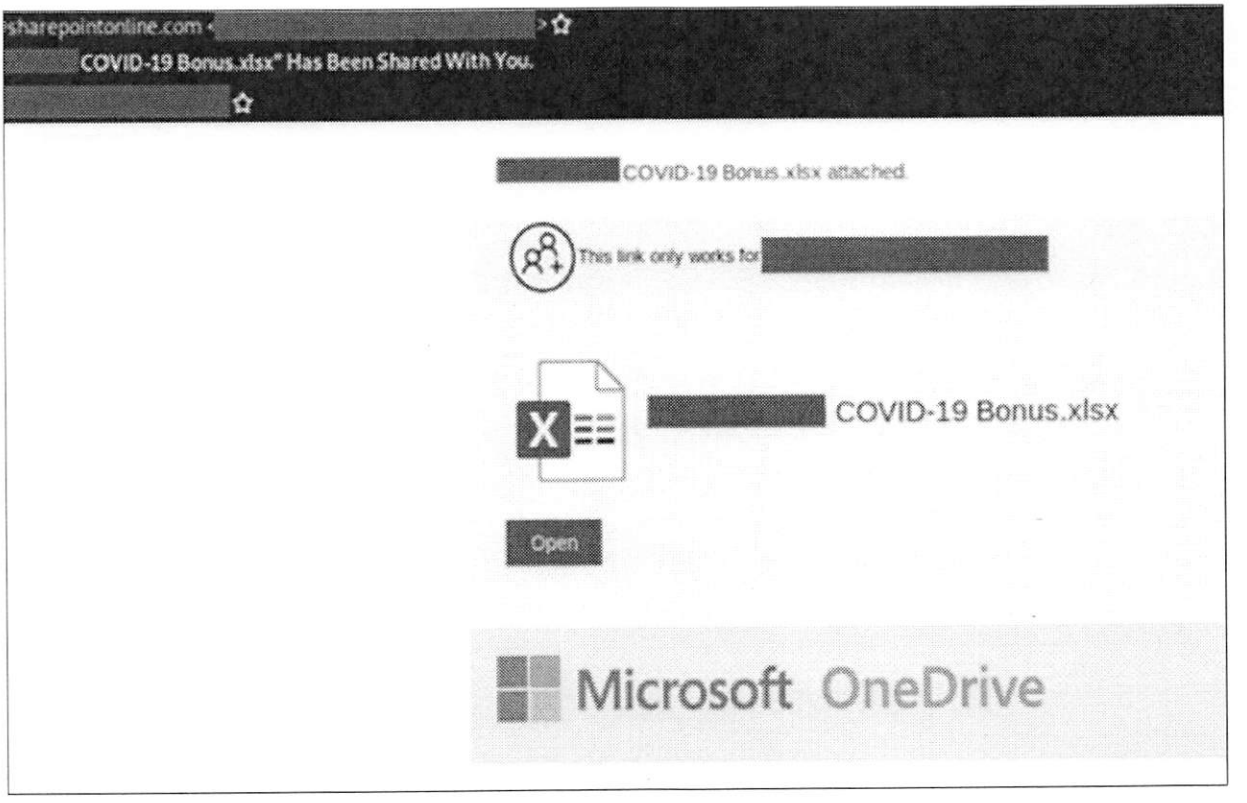

Figure 3

23. The scale of these phishing attacks is immense. In just one week, Defendants sent phishing emails to millions of Office 365 users. The scale of Defendants' attempts to reach potential victims and Defendants' ability to continuously create and deploy new malicious Web Apps from existing infrastructure demonstrates the substantial ongoing risk posed by Defendants.

Defendants Attempt to Access Office 365 Through Malicious Web Apps

24. After Defendants socially engineer the victim to click the link in the body of the email, the victim is then prompted to sign into Microsoft's legitimate Office 365 portal at login.microsoftonline.com. The login portal presented to the victim at this point is reflected at **Figure 4** below, where the victim enters their user name, and at **Figure 5**, where the victim enters their password:

Figure 4

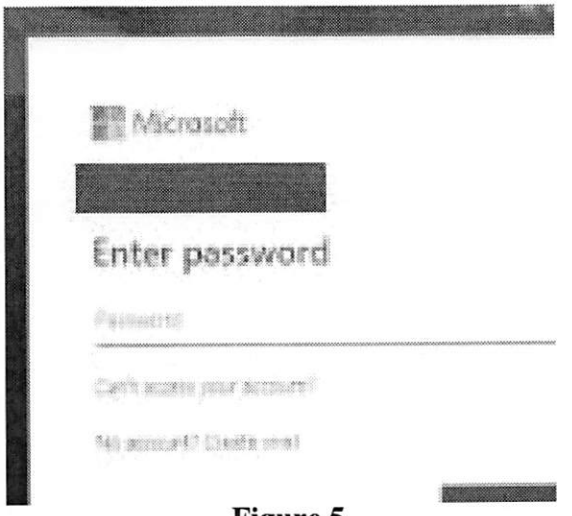

Figure 5

25. Once the Microsoft identity platform recognizes the credentials, the Defendants leverage an industry standard technical facility used by Microsoft known as "OAuth 2.0" to request access to victims' Office 365 accounts and to deceive victims into providing such access. The following describes the process by which Defendants misuse OAuth 2.0 to obtain access to victims' Office 365 accounts.

26. The first step in Defendants' misuse of OAuth 2.0 involves processing information contained within the URL that the Defendants used in the phishing email to take the victim to the legitimate Office 365 portal. That URL contains additional information that defines the level of access requested by the malicious Web App and to be granted by the unsuspecting

user. As seen in **Figure 6** the malicious URL contains several elements, highlighted below:

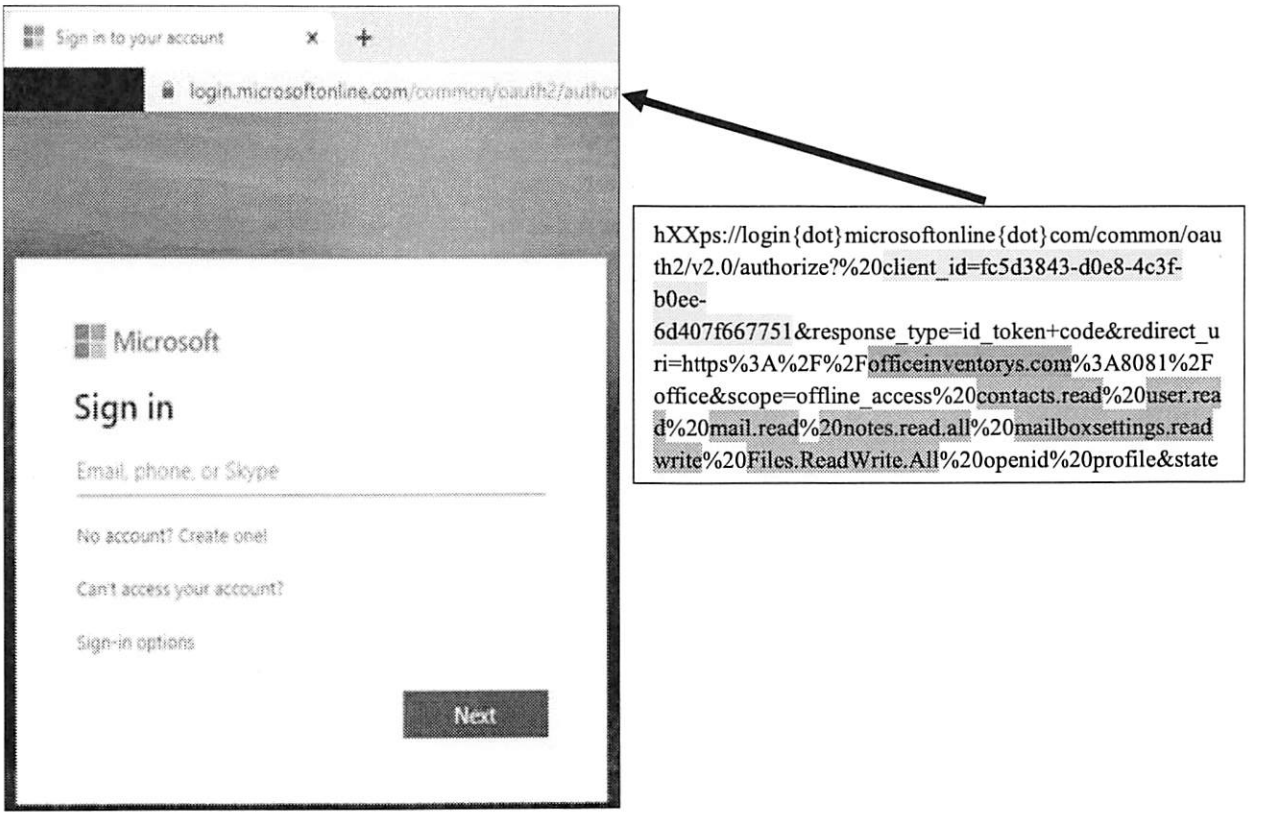

Figure 6

27. First, the malicious URL contains a parameter called **"client_id"** (highlighted in yellow above). The "client_id" is an identifier which is processed by the OAuth 2.0 facility to identify the Defendants' malicious Web App.

28. Second, the malicious URL contains a domain name, in this case "**officeinventorys.com**" (highlighted in green above). That is a domain name controlled by Defendants and one of the domain names that is the subject of this action. The Defendants' malicious Web App is hosted on servers associated with this domain name. In addition, once the user is deceived into accepting the Web App, authorization codes and/or tokens are sent to the servers associated with this domain name.

29. Third, the malicious URL contains other access parameters that operate as

instructions regarding what Office 365 resources to access. Highlighted in blue in the example above are parameters that define the level of access to Office 365 "**mail**," "**contacts**," "**files**" and "**notes**". Further, the parameters define access to "**read**" those resources and to "**write**" (*i.e.* make changes to) Office 365 mailbox settings and files. Access is only granted once the unsuspecting user accepts an OAuth 2.0 request, as discussed further below.

30. Upon login, the Defendants cause the OAuth 2.0 facility to use the "client_id" and the access parameters noted above to produce a deceptive user interface that displays the name of the malicious Web App and displays a list of access levels for which the malicious Web App is requesting consent. Defendants leverage this user interface in a manner that deceptively presents the trademark "Microsoft" and the deceptive formulation "0365," designed to look like the genuine Office 365. The deceptive Web App user interface, which the victim still believes to be an authorized process associated with a trusted entity (such as an employer), requests the victim to grant the following permissions regarding Office 365 access: read contacts, read user profile, read user emails, modify mailbox settings (i.e. forwarding rules) and all files. An example of a deceptive Web App user interface is shown at **Figure 7**.

Figure 7

31. After the user clicks "Accept," the OAuth 2.0 system generates an authorization code which is subsequently redeemed for one or more authentication tokens for that victim. This authentication token effectively serves the same function as the victim's credentials, communicating to the OAuth 2.0 system that the victim is authorized to have access to Office 365 account. In this way, the attacker is able to access the compromised Office 365 accounts by enabling the malicious Web App to gain access to the account in accordance with designated access parameters indicated in the graphical user interface depicted in Figure 7.

32. In this way, Defendants deceive victims to not only log into Office 365 and generate needed OAuth 2.0 tokens, but to further click on the "Accept" button, providing Defendants unauthorized access to defined resources within the Office 365 account. In this case, the victim will have granted access to all of the resources set forth above in Figure 6. Once Defendants deceive the victim into clicking "Accept," the OAuth 2.0 facility sends the previously generated OAuth 2.0 token and associated permissions to the Defendants' malicious Web App located at the Defendants' malicious domain name ("officeinventorys.com" in the example above). Once the malicious Web App receives the OAuth 2.0 token and associated permissions, this enables the Defendants to use the malicious Web App to make API calls to access the victim's Office 365 account. In accessing Microsoft's Office 365 servers in this way, Defendants are accessing, without valid authorization, computers that can be used in interstate commerce.

33. If Defendants were able to successfully access the content of Office 365 accounts pursuant to this phishing attack, it would be possible for them to carry out activities such as sending deceptive emails from the compromised user, monitoring communications and transactions in order to carry out wire fraud or other forms of fraud, or simply stealing further

financial credentials, account credentials or other valuable information that may be available. It is both the potential risk of Defendants' access to Microsoft's server resources, in general, and the potential risk of these further illegal activities that render the relief requested in this matter urgent and critical. All of the activities described above cause and threaten to cause serious injury to Microsoft and its customers. While Microsoft has taken additional technical measures to block this type of scheme, the Defendants are persistent and have attempted to circumvent those measures.

34. Defendants pose a current threat today and an ongoing threat into the future.

Defendants' Harmful Domain Names Used to Carry Out Attacks Against Microsoft Office 365 Accounts

35. Defendants use various domain names to host and deliver malicious Web Apps. Defendants have also registered domain names to prepare for other illegal activities, such as attempts to access the content of victims' emails. The following are domain names that Defendants are currently leveraging in their infrastructure, each of which is a .COM top-level domain (TLD) operated by Verisign as the Internet Corporation for Assigned Names and Numbers (ICANN) accredited registry within the Eastern District of Virginia.

Domain Names	Domain Registry	Registry Operator	Registry Location	Domain Registrar	Registrar Location
officeinventorys.com	.COM	Verisign	VA, United States	NameCheap, Inc.	AZ, United States
officehnoc.com	.COM	Verisign	VA, United States	NameCheap, Inc.	AZ, United States
officesuited.com	.COM	Verisign	VA, United States	NameCheap, Inc.	AZ, United States
officemtr.com	.COM	Verisign	VA, United States	NameCheap, Inc.	AZ, United States
officesuitesoft.com	.COM	Verisign	VA, United States	NameCheap, Inc.	AZ, United States
mailitdaemon.com	.COM	Verisign	VA, United States	GoDaddy.com, LLC	AZ, United States

36. As can be seen, many of these domain names are masquerades of Microsoft's

Office products and services, such as "officeinventorys.com", "officesuitesoft.com", and "officehnoc.com". This is consistent with the deceptive nature of the fraud targeting Office 365. These domain names are used to create malicious Web Apps, consistent with their deceptive theme. Defendants also registered the domain name "mailitdaemon.com," which has been and is used to receive mail forwarded by Office 365 accounts successfully compromised by Defendants. In this domain name, Defendants use generic nomenclature seen in regular network administration, such as "mail," "IT" (information technology) and "daemon" (a process used in an email server).

37. These domain names used by Defendants are identified in **Appendix A** to the Complaint.

Defendants' Trademark Infringement

38. In several different ways, Defendants deceive victims and disguise their malicious scheme by unauthorized reproduction of Microsoft's trademarks and brands. For example, as seen above and in **Appendix A**, Defendants have registered domains that leverage the term "office" associated with Microsoft's "Office 365" trademark, brand and services. Additionally, in the malicious phishing emails and Web App, Defendants reproduce the trademarks "Microsoft," the Microsoft corporate logo, "Office 365," "OneDrive," and "SharePoint," as well as confusingly similar variants such as "0365."

39. Further, Defendants have developed a technique where a victim clicking on a malicious link in a phishing email is first connected to the legitimate "microsoftonline.com" domain name. The victim clicks on the link, in reliance on deceptive information contained in the phishing email that causes the victim to mistakenly believe they are connecting to resources of a trusted entity such as an employer. This technique deceives and confuses victims into

thinking the link is not part of a malicious scheme because the domain name is owned by Microsoft and incorporates Microsoft's trademarks and branded material. Yet, unknown to the victim, the Defendants are delivering a malicious Web App that is not in fact affiliated with Microsoft or any other trusted entity. In these ways, Defendants' activities deceptively use Microsoft's trademarks and brands. Defendants' use of Microsoft trademarks and brands is meant to confuse Microsoft's customers into clicking on malicious links and clicking "Accept" in the deceptive Web App user interface, which they mistakenly believe are sponsored by Microsoft or trusted entities.

Harm to Microsoft

40. Microsoft® is a provider of the Office 365,® OneDrive,® and SharePoint® cloud-based business and productivity suite of services, all offered under those trademarks and in connection with the Microsoft mark and the Microsoft corporate logo. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Microsoft, Office 365, OneDrive and SharePoint trademarks.

41. Defendants use these trademarks, brands and confusingly similar variants in phishing emails and web interfaces presented to Microsoft's customers and potential victims. Defendants' use of Microsoft trademarks and brands is meant to confuse and does cause

confusion among Microsoft's customers and recipients of these communications, as those parties incorrectly perceive a relationship between Microsoft and the malicious activities of Defendants.

42. All of these activities cause injury to Microsoft. Customers expect Microsoft to provide safe and trustworthy products and services. There is a great risk that Microsoft's customers, both individuals and the enterprises they work for, may incorrectly attribute Defendants' malicious activities and the result of those activities, to Microsoft's products and services, should Defendants be able to carry out future attacks. Therefore, Defendants' activities dilute and tarnish the value of these Microsoft trademarks and brands. The activities carried out by Defendants, described above, injure Microsoft and its reputation, brand and goodwill because victims targeted by this scheme are likely to incorrectly believe that Microsoft is the source of problems caused by Defendants.

43. Microsoft is similarly injured because Defendants direct their attempted intrusions to accounts hosted on Microsoft's servers. Microsoft must bear this extraordinary burden. Microsoft must develop technical countermeasures and defenses, to suppress Defendants' activities, respond to customer service issues caused by Defendants and must expend substantial resources dealing with the injury and confusion. Microsoft has had to expend substantial resources to resist the ongoing attempted attacks on its infrastructure, products, services, and customers. Given that Defendants are continuing their targeting of Microsoft, and that such will be ongoing, this poses severe risk of injury to Microsoft, in that it ultimately threatens Microsoft's brands and customer relationships.

FIRST CLAIM FOR RELIEF

Violation of the Computer Fraud & Abuse Act, 18 U.S.C. § 1030

44. Microsoft incorporates by reference each and every allegation set forth above.

45. Defendants knowingly and intentionally accessed, continue to access and/or have attempted to access protected computers and networks of Microsoft and the online accounts of Microsoft's customers without authorization and knowingly caused and/or attempted to cause the transmission of a program, information, code and commands, resulting in damage to the protected computers and networks, the software residing thereon, and Microsoft.

46. Defendants' conduct involved interstate and/or foreign communications.

47. Defendants' conduct has caused a loss to Microsoft during a one-year period aggregating at least $5,000.

48. Microsoft seeks injunctive relief and compensatory and punitive damages under 18 U.S.C. §1030(g) in an amount to be proven at trial.

49. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SECOND CLAIM FOR RELIEF

Trademark Infringement Under the Lanham Act – 15 U.S.C. § 1114 *et seq.*

50. Microsoft incorporates by reference each and every allegation set forth above.

51. Defendants have used Microsoft's trademarks in interstate commerce, including Microsoft's federally registered trademarks for the marks "Microsoft," the Microsoft corporate logo, "Office 365," "OneDrive," and "SharePoint," among other trademarks.

52. As a result of their wrongful conduct, Defendants are liable to Microsoft for violation of the Lanham Act.

53. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

54. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

55. Defendants' wrongful and unauthorized use of Microsoft's trademarks to promote, market, or sell products and services constitutes trademark infringement pursuant to 15 U.S.C. § 1114 *et seq.*

THIRD CLAIM FOR RELIEF

False Designation of Origin Under The Lanham Act – 15 U.S.C. § 1125(a)

56. Microsoft incorporates by reference each and every allegation set forth above.

57. Microsoft's trademarks are distinctive marks that are associated with Microsoft and exclusively identify its businesses, products, and services.

58. Defendants make unauthorized use of Microsoft's trademarks. By doing so, Defendants create false designations of origin as to tainted Microsoft products that are likely to cause confusion, mistake, or deception.

59. As a result of their wrongful conduct, Defendants are liable to Microsoft for violation of the Lanham Act, 15 U.S.C. § 1125(a).

60. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

61. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

FOURTH CLAIM FOR RELIEF

Trademark Dilution Under The Lanham Act – 15 U.S.C. § 1125(c)

62. Microsoft incorporates by reference each and every allegation set forth above.

63. Microsoft's trademarks are famous marks that are associated with Microsoft and exclusively identify its businesses, products, and services.

64. Defendants make unauthorized use of Microsoft's trademarks. By doing so, Defendants are likely to cause dilution by tarnishment of Microsoft's trademarks.

65. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

66. As a direct result of Defendants' actions, Microsoft has suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

FIFTH CLAIM FOR RELIEF

Common Law Trespass to Chattels

67. Microsoft incorporates by reference each and every allegation set forth above.

68. Defendants have used a computer and/or computer network, without authority, with the intent to cause physical injury to the property of another.

69. Defendants have, without authority, used a computer and/or computer network of Microsoft and the online accounts of Microsoft's customers, without authority, with the intent to trespass on the computers, computer networks, and/or online accounts of Microsoft and its customers.

70. Defendants intentionally caused this conduct and this conduct was unlawful and unauthorized.

71. Defendants' actions have caused injury to Microsoft and have interfered with the possessory interests of Microsoft over its software, services, servers, and protected computers.

72. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

73. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SIXTH CLAIM FOR RELIEF

Conversion

74. Microsoft incorporates by reference each and every allegation set forth above.

75. Microsoft owns all right, title, and interest in its Office 365 software and services. Microsoft licenses its software to end-users. Defendants have interfered with, unlawfully and without authorization, and dispossessed Microsoft of control over its Office 365 software and services.

76. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to remove, halt, or otherwise disable or impair computer data, computer programs, and computer software from a computer or computer network.

77. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to cause a computer to malfunction.

78. Defendants have, without authority, dispossessed Microsoft of control over its computers and computer networks and have dispossessed Microsoft and its customers of control over online accounts.

79. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation the return of Defendants' ill-gotten profits.

80. As a direct result of Defendants' actions, Microsoft suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SEVENTH CLAIM FOR RELIEF

Unjust Enrichment

81. Microsoft incorporates by reference each and every allegation set forth above.

82. The acts of Defendants complained of herein constitute unjust enrichment of the Defendants at the expense of Microsoft in violation of the common law. Defendants used, without authorization, software belonging to Microsoft to facilitate unlawful conduct inuring to the benefit of Defendants.

83. Defendants profited unjustly from their unauthorized use of Microsoft's intellectual property.

84. Upon information and belief, Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of Microsoft's intellectual property.

85. Retention by the Defendants of the profits they derived from their malfeasance would be inequitable.

86. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten profits.

87. As a direct result of Defendants' actions, Microsoft suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays that the Court:

1. Enter judgment in favor of Microsoft and against the Defendants.

2. Declare that Defendants' conduct is willful and that Defendants acted with fraud, malice and oppression.

3. Enter a preliminary and permanent injunction enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein.

4. Enter a preliminary and permanent injunction giving Microsoft control over the domains used by Defendants to cause injury and enjoining Defendants from using such domains or any other similar instrumentalities.

5. Enter judgment awarding Plaintiff actual damages from Defendants adequate to compensate Plaintiff for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial.

6. Enter judgment disgorging Defendants' profits.

7. Enter judgment awarding enhanced, exemplary and special damages, in an amount to be proved at trial.

8. Enter judgment awarding attorneys' fees and costs, and

9. Order such other relief that the Court deems just and reasonable.

DEMAND FOR JURY TRIAL

Microsoft respectfully requests a trial by jury on all issues so triable in accordance with Fed. R. Civ. P. 38.

Dated: June 30, 2020

Respectfully submitted,

Julia Milewski (VA Bar No. 82426)
Matthew Welling (*pro hac vice*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
jmilewski@crowell.com
mwelling@crowell.com

Gabriel M. Ramsey (*pro hac vice*)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com

Attorneys for Plaintiff Microsoft Corporation